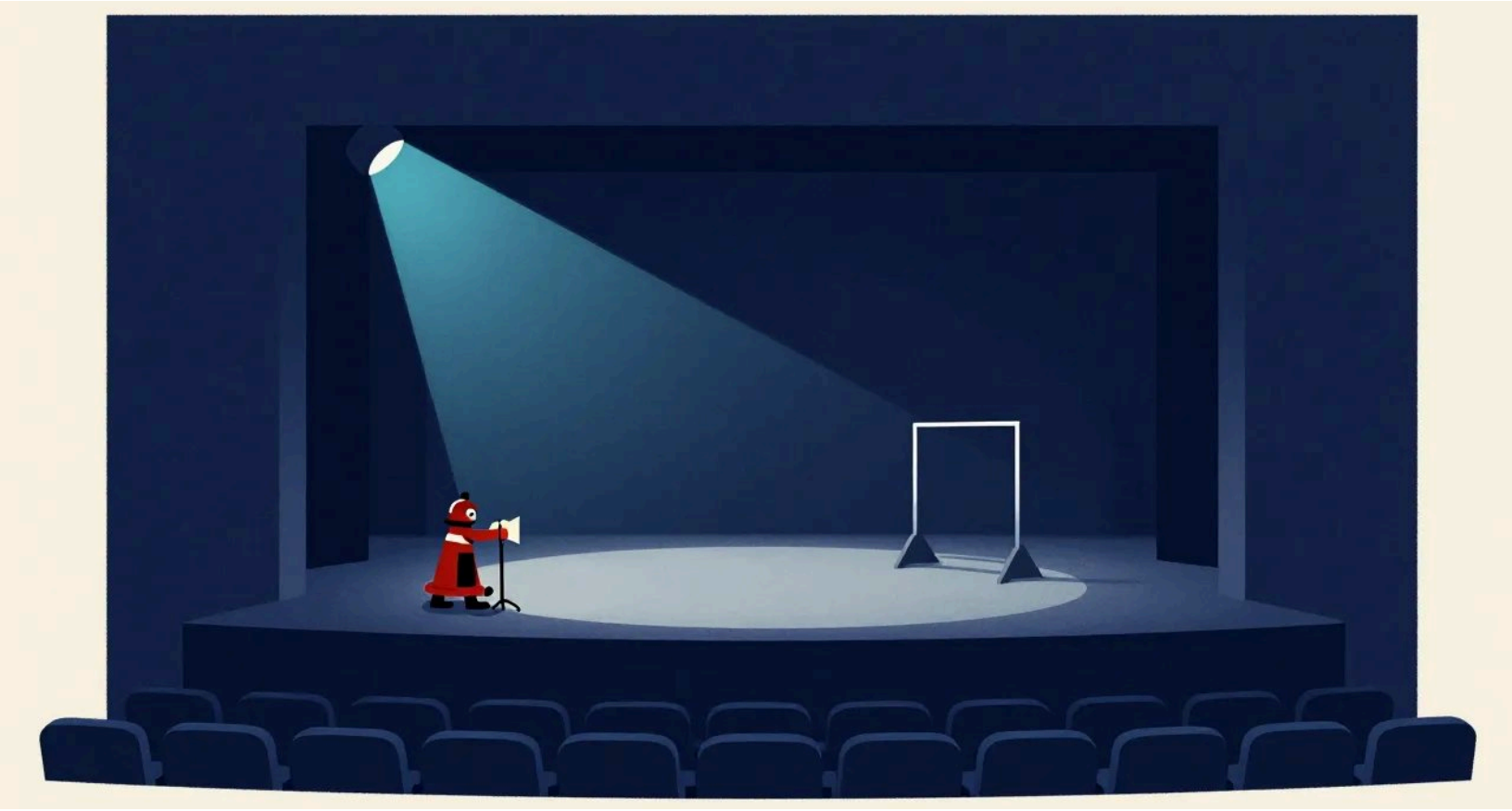


EXECUTIVE PAPER · DISASTER RECOVERY

Rehearse the Disaster Before It Happens

A recovery plan nobody has practiced tells you what the company intends to do. COOs and CTOs who exercise it learn what the company can actually do, while there is still time to close the gap.

AUTHOR

Chris Watkins

SERVICE

Disaster Recovery

FOR

COO, CTO · 11 min read

AT A GLANCE

The problem. Most companies have a written disaster recovery plan. Far fewer have watched their people carry it out under time pressure. The first real event becomes the first test, and the gaps show up as cancelled flights, lost records, and weeks of manual work.

Why it persists. Plans are written to satisfy auditors and then filed. Exercises take people away from projects, and a failed drill feels like bad news, so tests get scoped to pass. Dependencies such as identity systems, crew or staff scheduling, and outside vendors are assumed to be available.

The recommendation. Climb an exercise ladder every year: tabletop discussions for decision-makers, functional drills for the recovery team, and at least one live failover of a critical service. Write an after-action report for each, assign every finding an owner and a date, and report measured recovery times next to the targets in the plan.

The Decision in Front of You

A disaster recovery plan states how long each critical service may be down and how much data the business can afford to lose. Those targets go into contracts, board papers, and audit responses. Until someone has restored the service within the target, the numbers are estimates.

The decision for operations and technology leaders is whether to spend a few days of staff time each year proving the plan works, or to let the first real outage do it. Exercises cost money and attention, and the cases below show what the alternative cost two large organizations.

NIST's guidance on testing IT plans separates three activities [1][2]. Training tells people their roles. Exercises simulate an emergency to check whether the plan holds up. Tests use measurable results to confirm that a system or component works as the plan says. A recovery program needs all three.

What's Happening

Two recent cases where recovery set the cost

Delta Air Lines, July 2024. On July 19, 2024, a faulty security software update crashed Windows systems at airlines, banks, and hospitals worldwide. Delta cancelled about 7,000 flights over five days, affecting more than a million customers, while United cancelled about 1,500 [7]. Delta's chief executive put the cost at about $500 million [6]. The crew-tracking system that matches pilots and flight attendants to flights was crippled, and the airline had to reset 40,000 servers by hand [6][7]. Delta's pilot

and dispatcher unions said the crew scheduling system dates from the 1980s [7]. The U.S. Department of Transportation opened an investigation because Delta's recovery lagged its peers, and coverage in June 2026 reported the inquiry closed without major fines [8].

Delta's competitors were hit by the same update on the same morning [7]. What separated them was how fast each could rebuild its operation. For Delta, the bottleneck was a downstream business system that had to be repopulated and resynchronized after the computers came back. Public reporting does not say whether Delta had exercised a scenario like this one.

South Korea's government data center, September 2025. A battery fire on September 26, 2025, at the National Information Resources Service in Daejeon destroyed 96 systems and disrupted 647 [11]. Data submitted by the office of a National Assembly member showed that only 28 of the 647 systems at the site, 4.3%, had server-level disaster recovery that could switch to a standby server. Only 19 had replicated storage. None of the 96 destroyed systems had server-level recovery [10]. A shared document store used by government staff had no external backup at all, and its contents were reported as permanently lost [9]. In early October, 115 of the 647 systems were back, about 18%, and officials expected full recovery to take a month [11].

Almost all of the destroyed systems had backups [9][11]. What most of them lacked was a fast path back. A failover drill for each critical system would have produced a written list of the ones that could not fail over, while there was still time to fund the fixes.

Exercises expose what documents hide

Change Healthcare's 2024 ransomware attack is a third example. Its chief executive later told Congress that the primary and backup environments were not isolated from each other, so both were locked at once, and that cloud-hosted systems came back far faster than older data center systems [12]. A drill that tried to recover the backup environment without touching production would have shown the shared exposure.

Each case has the same shape. The plan assumed something would be available on the day: a scheduling system, a standby server, a separate backup environment. Nobody had proven it under realistic conditions.

Standards and regulators expect proof

NIST SP 800-84, the federal guide to test, training, and exercise programs for IT plans, calls for documenting each event in an after-action report and repeating exercises after organizational changes and plan updates [1][2]. Under NIST SP 800-53, federal agencies must exercise or test contingency and incident response plans at least once a year [2]. The CISA #StopRansomware Guide asks organizations to exercise their incident response plan regularly, keep hard copy and offline versions, and have the chief executive approve the plan in writing [5].

ISO 22301:2019, the international standard for business continuity management, requires exercises at planned intervals, based on realistic scenarios, that confirm the continuity arrangements work, produce formal post-exercise reports, and lead to improvement actions [13]. The FFIEC Business Continuity Management booklet, which replaced the earlier planning booklet in November 2019 and guides US bank examiners, treats testing as one of the core areas of an institution's continuity program [14]. In the European Union, the Digital Operational Resilience Act has applied to financial entities since January 17, 2025. It requires a resilience testing programme and testing at least once a year of the ICT systems that support critical or important functions [15]. Larger firms named by their supervisors must also run threat-led penetration testing at least every three years [16].

Why the Usual Approach Fails

Plans are written for an audience of auditors. The document describes the target state of recovery in careful language, gets signed, and goes into a repository. Nobody reads it until the event, and by then some of the names in the contact list belong to people who have changed jobs.

Tests are scoped to pass. Restoring one virtual machine from last night's backup proves the backup software works. It says nothing about restoring 200 servers in the right order while the identity system is down and the network team is on a bridge call with a vendor. Teams pick the easy test because a failed drill feels like a failing grade.

Tabletops stay in the conference room. A discussion exercise is valuable for decision-makers, and NIST is explicit that a tabletop deploys no equipment or resources [2]. It cannot reveal that a restore takes 14 hours instead of the four the plan promises. Only a functional drill can measure that.

The business process is left out. In the Delta case, the computers came back before the operation did [6][7]. Recovery plans written by IT usually end when the servers are up. Customers experience the end of the outage when orders ship, crews fly, or claims pay.

The plan lives inside the system that failed. If the runbook, the contact list, and the passwords sit on a file share that is encrypted or offline, the team starts the recovery from memory. CISA recommends keeping printed and offline copies for this reason [5].

Findings do not get fixed. An exercise that produces a list of gaps with no owners and no dates leaves those gaps in place for the next real event.

The Framework: The Exercise Ladder

Each type of exercise proves something the one below it cannot. A mature program climbs all the rungs every year and moves higher only after the lower rung runs cleanly.

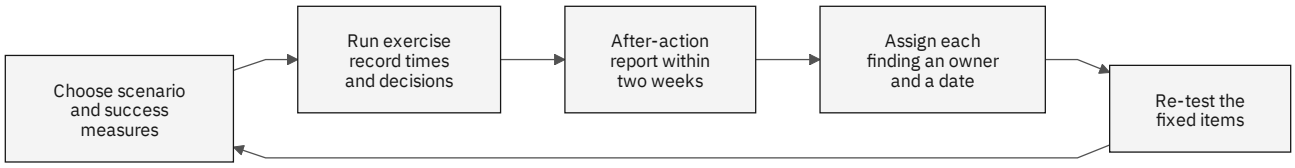
Exhibit 1. The exercise ladder: each rung proves something the one below it cannot

Rung	What happens	What it proves	What it cannot prove	Suggested frequency
1. Plan walkthrough	Owners read the plan and check contacts, access, and dependencies	The plan is current and people know their roles	That anything works	Quarterly
2. Tabletop exercise	Leaders talk through a scenario with a facilitator; no systems are touched [2]	Decisions, authority, and communications hold up	Recovery times	Twice a year, rotating scenarios
3. Functional drill	The recovery team restores a real service in an isolated environment, on the clock [2]	Measured recovery time and data loss for that service	Behavior under full production load and with the business involved	Each critical service once a year
4. Live failover	A critical service runs from its recovery site, with real users, for a set period	The business can operate on the recovery path	Every possible scenario	At least one critical service a year

Source: exercise types from NIST SP 800-84 [1][2]; frequencies are the author's recommendation.

The cycle around each exercise matters as much as the exercise.

Exhibit 2. Every exercise ends in owned fixes and a re-test



Source: author's framework, consistent with the after-action reporting in NIST SP 800-84 [1][2] and the after-action report and improvement plan templates in CISA's exercise packages [3][4].

Choose the scenario. Pick events the business has reason to fear: loss of a data center, ransomware in the directory service, a failed vendor update, a key supplier going dark. CISA publishes more than 100 tabletop exercise packages with ready-made scenarios, facilitator guides, discussion questions, and after-action report templates [3][4]. Set success measures before the exercise starts, using the recovery targets in the plan.

Run it with the business present. Invite the people who run the process that depends on the system: dispatch, customer service, finance, crew or shift scheduling. The exercise ends when the business process is running again, which can be well after the servers are.

Write it down. A short after-action report records what happened, how long each step took against the target, and what went wrong [1][2].

Fix and re-test. Every finding gets an owner, a due date, and a re-test. The report to leadership shows open findings by age, the same way audit findings are tracked.

Costs, Risks, and Tradeoffs

Exhibit 3. What a real exercise program costs, and when it is the wrong priority

Area	Cost or risk	Mitigation
Staff time	A functional drill can take a team two to five days including preparation and the report	Rotate services so each team drills once a year; schedule around peak periods
Business disruption	A live failover can cause a real outage if the recovery path is broken	Start with isolated drills; fail over in a low-traffic window with a tested rollback
Bad news	Early exercises will miss targets, and the results reach leadership	Agree in advance that a missed target becomes a finding with an owner, and that nobody is penalized for reporting it
Exercise theater	Scripted drills that always pass give false assurance	Introduce an unannounced complication; have someone outside the team observe
Finding backlog	Fixes compete with project work and stall	Report open findings by age to the COO; fund the largest fixes as projects
When this is wrong	A firm with no recovery site, no backups it controls, or no plan has nothing to exercise yet	Build the basic capability first; run only tabletops to set priorities and decide what to fund

Source: author's analysis.

How to Act

Exhibit 4. A one-year roadmap from written plan to proven capability

Window	Actions	Owner	Milestone
First 30 days	List critical services with their recovery time and data loss targets. Confirm the plan, contacts, and credentials are available offline and in print [5]. Record the date each service was last restored in a drill.	CTO with business service owners	Inventory complete, showing each service's last proven recovery date or "never"
First 30 days	Run a two-hour tabletop for the executive team using a CISA package or an internal scenario [3].	COO	After-action report issued; decision authority gaps listed with owners
First 90 days	Functional drill for the two most critical services in an isolated environment, timed against target, with the business process owner present.	Infrastructure or SRE lead	Measured recovery time and data loss for both services, reported against targets
First 90 days	Start a findings register with owners and dates; review it monthly.	COO's chief of staff or risk lead	Every finding has an owner and a due date
First 365 days	Functional drill for every critical service. One live failover of a critical service for at least one business day. Map results to the applicable standard or regulation.	CTO with internal audit	All critical services drilled within the year; one live failover completed; findings older than 90 days below an agreed number

Source: author's recommendation.

Questions to Ask Your Team

1. For each critical service, when did we last restore it in a drill, and how long did it take against the target?
2. Which services have no tested recovery path at all?
3. If the file share and email were down, where would the team find the plan and the contact list?
4. Which business systems, like scheduling or order management, have to be rebuilt after the servers come back, and is that time in our target?
5. What did our last exercise find, and how many of those findings are still open?
6. Who outside the recovery team watched the last drill?
7. Which outside vendors would we need on the phone in the first hour, and have they ever joined an exercise?

Closing

A recovery plan describes a capability the company hopes to have, and exercises measure how much of it exists. Climb the ladder each year, put the business process owners in the room, write down what broke, and fix it before the next drill. Report measured recovery times beside the targets, so leadership can see the distance between the plan and what the team can deliver on its worst day.

Sources

[1] National Institute of Standards and Technology. "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities." NIST SP 800-84. 2006. https://csrc.nist.gov/pubs/sp/800/84/final.

[2] National Institute of Standards and Technology. ITL Bulletin, December 2006, summarizing NIST SP 800-84. 2006. https://csrc.nist.gov/files/pubs/shared/itlb/itlbul2006-12.pdf.

[3] Cybersecurity and Infrastructure Security Agency. "CISA Tabletop Exercise Packages." https://cisa.gov/cisa-tabletop-exercises-packages.

[4] Cybersecurity and Infrastructure Security Agency. "CISA Tabletop Exercise Package (CTEP) Fact Sheet." 2020. https://www.cisa.gov/sites/default/files/publications/CTEP%20Fact%20Sheet%20v%2004.16.20_508.pdf.

[5] Cybersecurity and Infrastructure Security Agency, MS-ISAC, NSA, and FBI. "#StopRansomware Guide." Updated 2023. https://www.cisa.gov/stopransomware/ransomware-guide.

[6] NPR. "Delta's CEO says the CrowdStrike outage cost the airline $500 million in 5 days." 2024. https://www.npr.org/2024/07/31/nx-s1-5058652/delta-crowdstrike-outage-500-million-dollars.

[7] The Atlanta Journal-Constitution. "One year after travel meltdown, Delta-CrowdStrike dispute far from over." 2025. https://ajc-ajc-prod.cdn.arcpublishing.com/business/2025/07/one-year-after-travel-meltdown-delta-crowdstrike-dispute-far-from-over.

[8] Pulse. "Delta off the hook, avoids major fines as DOT ends 2-year probe into 2024 CrowdStrike chaos." Secondary coverage. 2026. https://www.pulse.bot/transportation/news/delta-off-the-hook-avoids-major-fines-as-dot-ends-2-year-probe-into-2024-crowdstrike-chaos-83598e7c-037d-43a5-94b3-49d3402586a3/.

[9] Korea JoongAng Daily. "NIRS fire destroys government's cloud storage system, no backups available." 2025. https://www.koreajoongangdaily.com/korea/nirs-fire-destroys-governments-cloud-storage-system-no-backups-available/12294122.

[10] Asia Economy. "NIRS Daejeon Headquarters: Server Disaster Recovery Rate Only 4.3%." 2025. https://www.asiae.co.kr/en/article/2025100119561436562.

[11] DatacenterDynamics. "858TB of government data may be lost for good after South Korea data center fire." 2025. https://www.datacenterdynamics.com/en/news/858tb-of-government-data-may-be-lost-for-good-after-south-korea-data-center-fire.

[12] Cybersecurity Dive. "Change Healthcare cyberattack: 5 technical takeaways from UnitedHealth CEO's testimony." 2024. https://www.cybersecuritydive.com/news/unitedhealth-change-attack-tech-takeaways/715200/.

[13] GlobalCert International. "ISO 22301 Exercising and Testing Program." Guide to ISO 22301:2019 clause 8.5. https://www.globalcertinternational.com/resources/guides/iso-22301-exercising-and-testing-program/.

[14] Office of the Comptroller of the Currency. "Business Continuity Management: Revised FFIEC Booklet." OCC Bulletin 2019-57. 2019. https://occ.treas.gov/news-issuances/bulletins/2019/bulletin-2019-57.html.

[15] Grant Thornton Ireland. "Digital Operational Resilience Act (DORA): Security Testing Requirements." https://www.grantthornton.ie/insights/factsheets/impact-of-dora-security-testing-requirements/.

[16] Regulation (EU) 2022/2554 (Digital Operational Resilience Act), Article 26, "Advanced testing of ICT tools, systems and processes based on TLPT." OJ L 333, 27.12.2022. Text via SpringLex. https://www.springlex.eu/en/packages/dora/dora-regulation/article-26/.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.